AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method of providing a circle of trust comprising:

receiving a first certificate of a first ~~affiliated entity~~ server by a second ~~affiliated entity~~ server;

storing said first certificate of said first ~~affiliated entity~~ server in a first trusted partner list accessible by said second ~~affiliated entity~~ server;

receiving a second certificate of said second ~~affiliated entity~~ server by said first ~~affiliated entity~~ server; and

storing said second certificate of said second ~~affiliated entity~~ server in a second trusted partner list accessible by said ~~second~~ first ~~affiliated entity~~ server [[;]],

wherein access by a client to a resource associated with said first server is controlled as a function of said first trusted partner list ~~or said second trusted partner list~~.

2. (Currently Amended) The method according to Claim 1 further comprising:

initiating use of [[a]] said resource ~~on a relying party device~~ by [[a]] said client ~~device~~, wherein an authentication assertion reference is provided by [[a]] said client ~~device~~;

determining an identity of ~~an~~ said second server ~~issuing party~~ as a function of said authentication assertion reference;

sending an authentication request containing [[a]] said first certificate of said first server ~~relying party~~ to said second server ~~issuing party~~;

determining if said first certificate is contained in [[a]] said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion indicating that said client has been authenticated, from said second server ~~issuing party~~ to said ~~relying party~~

first server when said first certificate is contained in [[a]] said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has not been authenticated, from said second server ~~issuing party~~ to said first server ~~relying party~~ when said first certificate is not contained in said first trusted partner list of said second server ~~issuing party~~; and

providing said ~~requested~~ resource to said client ~~device~~ by said first server ~~relying party~~ when said authentication assertion indicates that said client has been authenticated.

3. (Currently Amended) The method according to Claim 2, further comprising:

logging-on to said second server ~~issuing party utilizing~~ by said client ~~device~~; and

authenticating said client ~~device~~ by said second server ~~issuing party~~.

4. (Currently Amended) The method according to Claim 1, further comprising:

receiving a first network address of said first ~~affiliated entity~~ server by said second ~~affiliated entity~~ server;

storing said first network address of said first ~~affiliated entity~~ server in said first trusted partner list accessible by said second ~~affiliated entity~~ server;

receiving a second network address of said second ~~affiliated entity~~ server by said first ~~affiliated entity~~ server; and

storing said second network address of said second ~~affiliated entity~~ server in said second trusted partner list accessible by said first ~~second affiliated entity~~ server.

5. (Currently Amended) The method according to Claim 4, further comprising:

initiating ~~user~~ use of [[a]] said resource ~~on a relying party device~~ associated with said first server by [[a]] said client ~~device~~, wherein an authentication assertion reference is provided by ~~a~~ said client ~~device~~;

determining an identity of said second server ~~an issuing party~~ as a function of said authentication assertion reference;

sending an authentication request from said first server ~~a relying party~~ to said second server ~~an issuing party~~;

determining [[a]] said first network address of said ~~relying party~~ first server from said authentication request;

determining if said first network address is contained in [[a]] said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has been authenticated, from said second server ~~issuing party~~ to said ~~relying party~~ first server when said first network address is contained in [[a]] said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has not been authenticated, from said second server ~~issuing party~~ to said ~~relying party~~ first server when said first network address is not contained in said first trusted partner list of said second server ~~issuing party~~; and

providing said ~~requested~~ resource to said client ~~device~~ by said first server ~~relying party~~ when said authentication assertion indicates that said client has been authenticated.

6. (Original) The method according to Claim 4, wherein said first network address and said second network address comprises a first and second internet protocol (IP) address respectively.

7. (Currently Amended) The method according to Claim 1, further comprising:

receiving a first network address of a third ~~affiliated entity~~ server by said first ~~affiliated entity~~ server;

storing said first network address of said third ~~affiliated entity~~ server in said second trusted partner list accessible ~~accessable~~ by said first ~~affiliated entity~~ server;

receiving a second network address of said first ~~affiliated entity~~ server by said third ~~affiliated entity~~ server; and

storing said second network address of said first ~~affiliated entity~~ server in a third trusted partner list accessible ~~accessable~~ by said third ~~affiliated entity~~ server.

8. (Currently Amended) A method of providing a circle of trust comprising:

initiating ~~user~~ use of a resource associated with ~~on~~ a relying ~~party~~ server ~~device~~ by a client ~~device~~, wherein an authentication assertion reference is provided by said ~~a~~ client to said relying server, ~~device~~ and wherein said authentication assertion reference is provided to said client by an issuing server;

determining an identity of [[an]] said issuing ~~party~~ server as a function of said authentication assertion reference;

sending [[an]] a first authentication request comprising ~~containing~~ a certificate of said relying ~~party~~ server to said issuing ~~party~~ server;

determining if said certificate is contained in a trusted partner list of said issuing ~~party~~ server;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing ~~party~~ server to said relying ~~party~~ server when said certificate is contained in [[a]] said trusted partner list of said issuing ~~party~~ server;

sending an authentication assertion, indicating that said client has not been authenticated, from said issuing ~~party~~ server to said relying ~~party~~ server when said certificate is not contained in said trusted partner list of said issuing ~~party~~ server; and

providing said ~~requested~~ resource to said client ~~device~~ by said relying ~~party~~ server when said authentication assertion indicates that said client has been authenticated.

9. (Currently Amended) The method according to Claim 8, further comprising:

sending [[an]] a second authentication request from said relying ~~party~~ server to said issuing ~~party~~ server;

determining a network address of said relying ~~party~~ server from said second authentication request;

determining if said network address is contained in [[a]] said trusted partner list of said issuing ~~party~~ server;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing ~~party~~ server to said relying ~~party~~ server when said network address is contained in [[a]] said trusted partner list of said issuing ~~party~~ server;

sending an authentication assertion, indicating that said client has not been authenticated, from said issuing ~~party~~ server to said relying ~~party~~ server when said network address is not contained in said trusted partner list of said issuing ~~party~~ server; and

providing said requested resource to said client ~~device~~ by said relying ~~party~~ server when said authentication assertion indicates that said client has been authenticated.

10. (Currently Amended) The method according to Claim 9, wherein said ~~first~~ network address ~~and said second network address comprise a first and second~~ comprises an internet protocol (IP) address ~~respectively~~.

11. (Currently Amended) The method according to Claim 8, further comprising:

logging-on to an issuing ~~party~~ server ~~utilizing~~ by said client ~~device~~; and

authenticating said client ~~device~~ by said issuing ~~party~~ server.

12. (Currently Amended) A system for providing a circle of trust comprising:

a first ~~affiliated entity~~ server comprising[[;]]:

a first administration module; and

a first trusted partner list communicatively coupled to said first administration module; and

~~said~~ a second ~~affiliated entity~~ server comprising[[;]]:

a second administration module; and

a second trusted partner list communicatively coupled to said second administration module,

wherein access by a client to a resource associated with said first server is controlled as a function of said second trusted partner list.

13. (Currently Amended) The system for providing a circle of trust according to claim 12, wherein said first administration module receives ~~said~~ a credential of said second ~~affiliated entity~~ server.

14. (Currently Amended) The system for providing a circle of trust according to claim 13, wherein said first administration module stores said credential of said second ~~affiliated entity~~ server in [[a]] said first trusted partner list.

15. (Original) The system for providing a circle of trust according to Claim 14, wherein said credential comprises a certificate.

16. (Original) The system for providing a circle of trust according to Claim 14, wherein said credential comprises a network address.

17. (Currently Amended) The system for providing a circle of trust according to Claim ~~13~~12, ~~further comprising:~~

[[a]] said client ~~device~~;

[[a]] said first ~~affiliated entity~~ server communicatively coupled to said client and ~~a~~ said second ~~affiliated entity~~ server, ~~comprising~~wherein said first server further comprises:[[;]]

a first session module; and

a first authentication module; and

said second ~~affiliated entity~~ server communicatively coupled to said client ~~device~~ and said first ~~affiliated entity~~ server, ~~comprising~~wherein said second server further comprises:[[;]]

a second session module; and

~~a second trusted partner list~~a second authentication module.

18. (Currently Amended) The system for providing a circle of trust according to Claim 17, wherein said second session module determines ~~the~~ an identity of said first server ~~an issuing party~~ as a function of an authentication assertion reference received from said client ~~device~~.

19. (Currently Amended) The system for providing a circle of trust according to Claim 17, wherein said first session module determines a trusted status of said second ~~affiliated entity~~ server as a function of a certificate received from said second session module.

20. (Currently Amended) The system for providing a circle of trust according to Claim 17, wherein said first session module determines a trusted status of said second ~~affiliated entity~~ server as a function of a network address of said second session module.

21. (Canceled)

22. (Currently Amended) The system for providing a circle of trust according to Claim 17 ~~21~~, wherein said first session module provides for secure transfer of information for authenticating ~~a user on~~ said client ~~device~~.

23. (Original) The system for providing a circle of trust according to Claim 22, wherein said first session module generates and processes SAML requests and assertions contained in SOAP envelopes.

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Currently Amended) The system for providing a circle of trust according to Claim 20 ~~21~~, wherein said first session module determines said network address of said second session module from an HTTP header.

28. (Currently Amended) A computer readable-medium containing a plurality of instructions which when executed ~~cause a network device to~~ implement a method of providing a circle of trust comprising:

receiving a first network address of a first ~~affiliated entity~~ server by a second ~~affiliated entity~~ server;

storing said first network address of said first ~~affiliated entity~~ server in a first trusted partner list ~~accessable~~ accessible by said second ~~affiliated entity~~ server;

receiving a second network address of said second ~~affiliated entity~~ server by said first ~~affiliated entity~~ server; and

storing said second network address of said second ~~affiliated entity~~ server in a second trusted partner list accessible ~~accessable~~ by said first ~~second affiliated entity~~ server,

wherein access by a client to a resource associated with said first server is controlled as a function of said first trusted partner list.

29. (Currently Amended) The computer readable-medium according to Claim 28, further comprising:

initiating use of [[a]] said resource ~~on a relying party device~~ associated with said first server by [[a]] said client ~~device~~, wherein an authentication assertion reference is provided by [[a]] said client ~~device~~;

determining an identity of ~~an issuing party~~ said second server as a function of said authentication assertion reference;

sending an authentication request from said first server ~~a relying party~~ to said second server ~~an issuing party~~;

determining [[a]] said first network address of said ~~relying party~~ first server from said authentication request;

determining if said first network address is contained in [[a]] said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has been authenticated, from said second server ~~issuing party~~ to said ~~relying party~~ first server when said first network address is contained in [[a]] said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has not been authenticated, from said second server ~~issuing party~~ to said ~~relying party~~ first server when said first network address is not contained in said first trusted partner list of said second server ~~issuing party~~; and

providing said ~~requested~~ resource to said client ~~device~~ by said first server ~~relying party~~ when said authentication assertion indicates that said client has been authenticated.

30. (Currently Amended) The computer readable-medium according to Claim 28, further comprising:

receiving a first certificate of ~~a~~ said first ~~affiliated entity~~ server by ~~a~~ said second ~~affiliated entity~~ server;

storing said first certificate of said first ~~affiliated entity~~ server in said first trusted partner list ~~accessable~~ accessible by said second ~~affiliated entity~~ server;

receiving a second certificate of said second ~~affiliated entity~~ server by said first ~~affiliated entity~~ server; and

storing said second certificate of said second ~~affiliated entity~~ server in said second trusted partner list ~~accessable~~ accessible by said first ~~second affiliated entity~~ server.

31. (Currently Amended) The computer readable-medium according to Claim 30, further comprising:

sending an authentication request containing ~~a~~ said first certificate of said first server ~~relying party~~ to said second server ~~issuing party~~;

determining if said first certificate is contained in a first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has been authenticated, from said second server ~~issuing party~~ to said first server ~~relying party~~ when said first certificate is contained in said first trusted partner list of said second server ~~issuing party~~;

sending an authentication assertion, indicating that said client has not been authenticated, from said second server ~~issuing party~~ to said first server ~~relying party~~ when said first certificate is not contained in said first trusted partner list of said second server ~~issuing party~~; and

providing said ~~requested~~ resource to said client ~~device~~ by said first server ~~relying party~~ when said authentication assertion indicates that said client has been authenticated.

32. (Currently Amended) The computer readable-medium according to Claim 31, further comprising:

logging-on to said second server by ~~issuing party utilizing~~ said client ~~device~~; and

authenticating said client ~~device~~ by said second server ~~issuing party~~.

33. (New) A method of providing a circle of trust comprising:

initiating use of a resource associated with a relying server by a client, wherein an authentication assertion reference is provided by said client;

determining an identity of an issuing server as a function of said authentication assertion reference;

sending an authentication request from said relying server to said issuing party;

determining a network address of said relying server from said authentication request;

determining if said network address is contained in a trusted partner list of said issuing server;

sending an authentication assertion, indicating that said client has been authenticated, from said issuing server to said relying server when said network address is contained in said trusted partner list of said issuing server;

sending an authentication assertion, indicating that said client has not been authenticated, from said issuing server to said relying server when said network address is not contained in said trusted partner list of said issuing server; and

providing said resource to said client by said relying server when said authentication assertion indicates that said client has been authenticated.

34. (New) The method according to Claim 33, further comprising:

logging-on to an issuing server by said client; and

authenticating said client by said issuing server.

35. (New) The computer readable-medium according to Claim 28, further comprising:

receiving said first network address of said first server by a third server;

storing said first network address of said first server in a third trusted partner list accessible by said third server;

receiving a third network address of said third server by said first server; and

storing said third network address of said third server in said second trusted partner list accessible by said first server.

36. (New) The method according to Claim 1, further comprising:

receiving said first certificate of said first server by a third server;

storing said first certificate of said first server in a third trusted partner list accessible by said third server;

receiving a third certificate of said third server by said first server; and

storing said third certificate of said third server in said second trusted partner list accessible by said first server,

wherein access by said client to said resource associated with said first server is controlled as a function of said third trusted partner list.